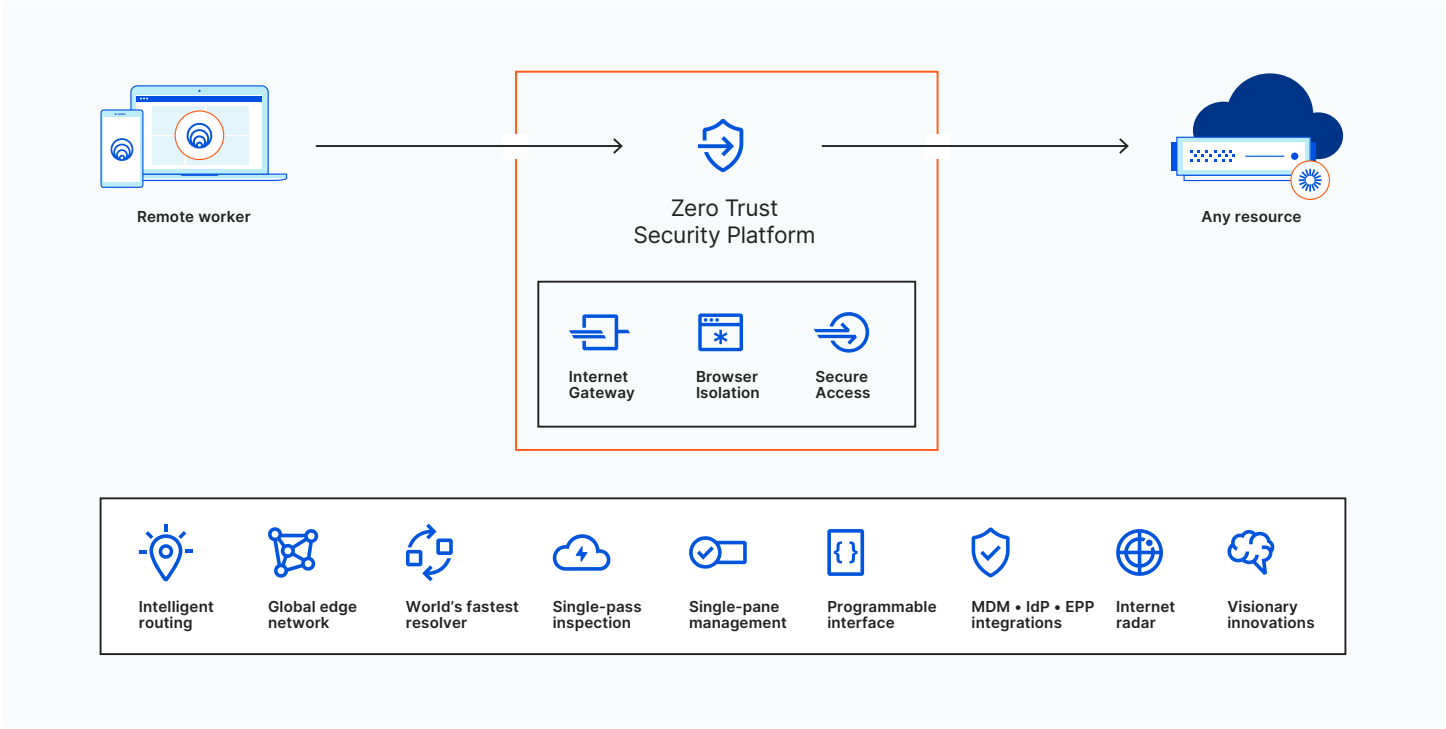
Securing remote worker connectivity for the long haul with Cloudflare

When COVID-19 forced an overnight transition to remote work, businesses scrambled to keep employees connected. Some solutions were strategic, but others were tactical bandaids — like doubling down on slow and unreliable VPNs, split-tunneling Internet traffic, and applying hasty remote access hacks. Now the cracks in this approach are showing, as familiar challenges with visibility, security and complexity persist.

Fixing remote work security flaws shouldn't take months or weeks. With Cloudflare's Zero Trust security platform, administrators can address over 20 pressing workforce security and connectivity use cases in just 30 minutes.

The solution: Cloudflare for Teams



Cloudflare's Zero Trust security platform increases visibility, eliminates complexity, and reduces risks as remote workers connect to applications and the Internet. It runs on the world's fastest edge network to deploy faster and perform better than other providers.

Three ways a Zero Trust platform can enhance remote worker security

Reduce risks

Reliance on VPNs has created failover risk and has left holes in corporate infrastructure for attackers to exploit. Once an attacker gains access, they can move laterally across multiple resources to steal data. Despite best efforts to block and tackle threats, endpoints still get compromised by undiscovered malware.

Zero Trust security platforms reduce remote work risks by enforcing identity and context-based authentication on every request to your corporate apps, leaving little room for lateral movement. Browser Isolation isolates endpoints from browsing activity, mitigating known and unknown threats.

Increase visibility

It was straightforward to maintain activity logs when users were in the office, but maintaining an audit trail is much more difficult when employees are geographically distributed and working from new devices. Logging capabilities within SaaS applications are often inconsistent, and VPN logs can be difficult to parse.

Zero Trust platforms restore visibility by intercepting and logging requests from all remote devices — even unmanaged devices. Administrators can monitor remote worker activity in internally-hosted and SaaS apps, with an audit trail to investigate incidents. Logs are centralized in one dashboard, and automatically sent to the SIEM of choice.

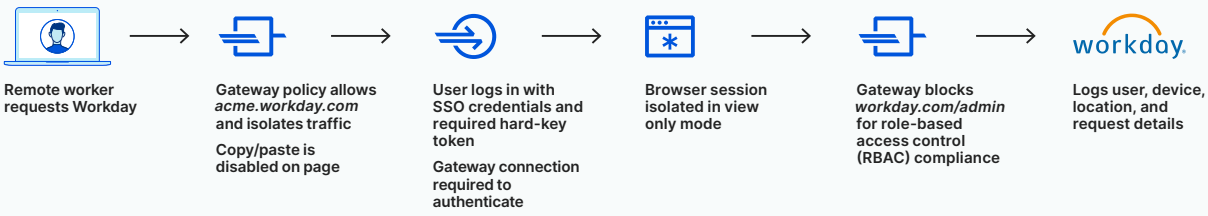
Eliminate complexity

Band-aid solutions implemented to connect remote workers are proving to be too fragile for the long run. Administrators are left to manage traffic filtering policies across multiple incompatible tools, and users are frustrated by the sluggish performance.

Zero Trust platforms simplify how users connect, and streamline how administrators work. With reduced reliance on legacy VPNs, administrators can apply standard security controls to all traffic - regardless of how that connection starts or where in the network stack it lives. And policies can all be managed from one dashboard.

Zero Trust security in action

Use case: prevent data loss in SaaS applications



In a single-pass architecture, remote worker traffic is inspected, isolated, logged, and secured from Internet threats; and performance never suffers, as users connect to data centers just one short hop nearby.

6 critical remote work problems solved

Use Case	How
Connect remote workers to corporate apps	Between devices and apps, route traffic (DNS, HTTP(S), RDP/SSH) through Cloudflare's network for better performance and reliability than your VPN
Adopt Zero Trust security for app access	Enforce application access policies based on identity, device posture and context (geo) instead of network location (IP)
Adopt Zero Trust security for internet browsing	Isolate browser activity from protected devices to stop malware and phishing from compromising endpoints
Protect data from unauthorized access and uploads	Exert finer-grained control over user and device access rights; prevent file uploads/downloads, copy/paste
Protect devices from malicious content within a site	Any known or unknown malicious content runs remotely in safe containers across our network, isolating it from reaching the device's local browser
Protect users from phishing sites	Native and third-party threat intel blocks phishers before they strike

Key Results

80%↓

less time spent resolving IT tickets and security posture for remote workers

30 min

to achieve the first two steps to Zero Trust security

91%↓

decrease in attack surface by placing Cloudflare in front of application access and Internet browsing

Next steps

Watch the demo

Try Teams, free for up to 50 users

Request a live demo with a Cloudflare expert